

ABSTRACT

The present invention generates watermark from ID information that uniquely identifies a program
5 distribution destination, inserts the generated watermark in a program, and prevents the program from operating correctly if the watermark is tampered with, and also inserts the same watermark verification code in a program regardless of the distribution destination.
10 By this means, it is possible to prevent detection of watermark verification code constituting a watermark by means of collusion attack.